DATA SHEET

CISCO ASA SOFTWARE VERSION 7.0

Cisco® ASA 5500 Series adaptive security appliances deliver numerous market-leading, high-performance security and VPN services for small and medium-sized businesses (SMBs), enterprises, and service providers—in addition to providing unprecedented services flexibility and extensibility and lower deployment and operations costs.

PRODUCT OVERVIEW

Cisco® ASA 5500 Series adaptive security appliances are purpose-built solutions that combine best-of-breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting SMBs and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

The Cisco ASA 5500 Series delivers a powerful combination of multiple market-proven technologies in a single platform, making it operationally and economically feasible to deploy comprehensive security services to more locations. And its multifunction security profile virtually eliminates the difficult—and risky—decision of making trade-offs between robust security protection and the operational costs associated with multiple devices in numerous locations.

The Cisco ASA 5500 Series helps businesses more effectively and efficiently protect their networks while delivering exceptional investment protection through the following key elements:

- **Market-proven security and VPN capabilities**—Full-featured, high-performance firewall, intrusion prevention system (IPS), network antivirus, and IP Security/Secure Sockets Layer (IPSec/SSL) VPN technologies deliver robust application security, user- and application-based access control, worm and virus mitigation, malware protection, and remote user and site connectivity.
- **Extensible Adaptive Identification and Mitigation services architecture**—Taking advantage of a modular services processing and policy framework, the Cisco Adaptive Identification and Mitigation architecture enables the application of specific security or network services on a per traffic flow basis, delivering highly granular policy controls and anti-x protection with streamlined traffic processing. The efficiencies of the Cisco ASA 5500 Series AIM architecture, as well as software and hardware extensibility through user-installable security services modules (SSMs), advance the evolution of existing services as well as deployment of new services without requiring a platform replacement or performance compromise. As the architectural foundation of the Cisco ASA 5500 Series, AIM enables highly customizable security policies and unprecedented services extensibility to help protect against the fast-evolving threat environment.
- **Reduced deployment and operations costs**—These multifunction appliances allow for platform, configuration, and management standardization, helping decrease the costs of deployment and ongoing operations.

MARKET-PROVEN SECURITY AND VPN CAPABILITIES

The Cisco ASA 5500 Series leverages Cisco's expertise in developing industry-leading and award-winning security and VPN solutions, and integrates the latest technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Intrusion Prevention Systems, and Cisco VPN 3000 Series Concentrators. By combining these technologies, the Cisco ASA 5500 Series delivers an unmatched, best-of-breed solution that stops the broadest range of threats and provides businesses with flexible, secure connectivity options. The breadth and depth of security and networking services provided by the Cisco ASA 5500 Series enable it to protect any area of the network, including the most common threat vectors such as mobile users, remote sites, and unmanaged desktops and servers. As a key component of the Cisco Adaptive Threat Defense and flexible

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

secure connectivity strategies, these security appliances converge a wide range of security and VPN technologies to provide rich application security, anti-x defenses, network containment and control, and secure connectivity.

APPLICATION SECURITY

The Cisco ASA 5500 Series provides strong application layer security through 30 intelligent, application-aware inspection engines that examine network flows at Layers 2–7. To defend networks from application layer attacks and give businesses control over use of applications and protocols in their environments, these inspection engines incorporate extensive application and protocol knowledge and employ security enforcement technologies that include application and protocol command filtering, protocol anomaly detection, and application and protocol state tracking. As another layer of application inspection and control, these inspection engines also incorporate attack detection and mitigation techniques such as buffer overflow defenses, content filtering and verification, and URL deobfuscation services. Inspection engines are available for a wide range of popular applications and protocols, including Web, file transfer, e-mail, voice and multimedia, database, operating system, and third-generation (3G) Mobile Wireless services. These inspection engines also give businesses control over threats such as instant messaging, peer-to-peer file sharing, and other tunneling applications, allowing businesses to enforce usage policies and protect network bandwidth for legitimate business applications.

ANTI-X DEFENSES

The Cisco ASA 5500 Series provides advanced, high-performance protection against network and application layer attacks, denial-of-service (DoS) attacks, and malware, including worms, network viruses, Trojan horses, spyware, and adware. Effective anti-x defense requires broad attack detection coupled with advanced analysis techniques, resulting in highly accurate threat classification that helps ensure appropriate mitigation actions are taken with no impact on legitimate network traffic.

Advanced Detection Techniques

To help ensure that threats do not go unnoticed, the Cisco ASA 5500 Series offers numerous methods to identify policy violations, anomalous activity, and vulnerability exploitation. They include stateful pattern recognition for stopping attacks hidden inside a data stream; protocol analysis to validate network traffic; traffic anomaly detection to identify attacks that cover multiple sessions and connections; protocol anomaly detection to identify attacks based on observed deviations in the normal RFC behavior of a protocol or service; and Layer 2 analysis to detect man-in-the-middle attacks. Specialized safeguards “scrub” network traffic to prevent “detection evasion” attempts; these safeguards include IP fragmentation reassembly and normalization, TCP stream reassembly and normalization, TCP evasion control, IP antispoofing, and deobfuscation.

Combined with the extensive detection techniques are two innovative analysis and correlation technologies from Cisco Systems® that help enable accurate mitigation of the detected threats: Risk Rating and the Meta Event Generator.

Risk Rating

The Cisco ASA 5500 Series uses the innovative Cisco Risk Rating technology to help ensure that malicious attacks are stopped without impacting legitimate traffic. Going beyond the typical single-factor methods in determining threat risk, Cisco Risk Rating incorporates four measures to accurately determine the risk of an event:

- **Event severity**—Rating indicating the relative impact of the threat
- **Signature fidelity**—Rating indicating the accuracy of the signature
- **Asset value**—Customizable value indicating the importance of the attack target (low value for a print server in a wiring closet, a high value for an e-commerce server in a data center, for example)
- **Attack relevancy**—Value based on susceptibility of the target to the attack type

These four factors combine to produce an accurate threat rating that allows for confident mitigation actions to take place.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Cisco Meta Event Generator

To quickly and accurately identify and stop worms that can rapidly propagate and cause extensive damage, the Cisco ASA 5500 Series includes Cisco Meta Event Generator technology, which provides unique on-device correlation capabilities. This is achieved through real-time modeling of worm behavior, including correlation of multiple event types and the time between individual events. As worms attempt to move through a network, they propagate through the transmission of multiple packets, which in many cases appear to be legitimate traffic. The generator uses its real-time correlation services to identify the initial packets associated with worm propagation and stops the follow-on packets necessary to complete the worm infestation. Thus the worm cannot reach the intended target intact so is, in fact, ineffectual.

SECURE CONNECTIVITY SERVICES

The Cisco ASA 5500 Series provides robust site-to-site and remote-access VPN services, enabling businesses to create secure connections across public networks to mobile users, remote sites, and business partners. An integrated approach to security is provided, enabling organizations to gain the connectivity and cost benefits of the Internet, without compromising the integrity of the corporate security policy.

By integrating VPN services with the wide range of security services offered by the Cisco ASA 5500 Series, businesses benefit from a stronger, more secure VPN connectivity. Integrated Cisco Adaptive Threat Defense capabilities help ensure that VPNs do not become a conduit for network attacks such as worms, viruses, malware, or hacking. Detailed application and access control policies can also be applied to VPN traffic, so individuals and groups of users have access only to the services and resources to which they are entitled. Additionally, customized quality-of-service (QoS) policies can be applied on a per-user, -group, -tunnel, or -flow basis, helping ensure that the appropriate priority and bandwidth restrictions are applied to specific network traffic flows.

Remote-Access VPN

The Cisco ASA 5500 Series offers flexible technologies that deliver tailored solutions to suit connectivity requirements, providing employees' company-managed desktops with robust, customizable remote access through an IPSec VPN. For situations where endpoints are not company-managed, such as extranets, Internet kiosks, or employee-owned desktops, the Cisco ASA 5500 Series delivers WebVPN for SSL-based remote access. Taking advantage of Cisco remote-access expertise, enterprises can deploy a single, integrated platform with broad support for core enterprise applications.

- **Flexible platform**—Offers both IPSec and SSL-based VPN services on a single platform, eliminating the need to provide parallel solutions. The Cisco ASA 5500 Series eliminates the inefficiencies and added costs of deploying separate, distinct platforms for both SSL and IPSec VPNs.
- **Resilient clustering**—Allows remote-access deployments to scale cost-effectively by evenly distributing VPN sessions across Cisco ASA 5500 Series and Cisco VPN 3000 Series platforms without requiring any user intervention. This highly resilient capability eliminates any single point of failure, allows businesses to scale their VPN headends as needed, and gives businesses excellent investment protection.
- **Cisco Easy VPN**—Delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Cisco ASA 5500 Series appliances dynamically push the latest VPN security policies to remote VPN devices and clients, helping ensure that those remote endpoints have up-to-date policies in place before the connection is established, thereby offering the ultimate flexibility, scalability, and ease of use. Furthermore, the Cisco ASA 5500 Series provides VPN client software with "auto-update" capabilities that help enable automated version upgrades for Cisco VPN Client software operating on remote desktops.

Site-to-Site VPN

Using the standards-based site-to-site VPN capabilities provided by the Cisco ASA 5500 Series, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide.

- **VPN infrastructure for today's applications**—The Cisco ASA 5500 Series provides a VPN infrastructure capable of converged voice, video, and data across a secure IPSec network, by combining robust site-to-site VPN support with rich inspection capabilities, QoS, dynamic routing, and stateful failover features, allowing businesses to take advantages of the many benefits of converged networks.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

- **Robust security and performance**—Branch and remote offices extend a company's reach into important markets and locations. Cisco ASA 5500 Series-based VPN solutions help enable secure, high-speed communications between multiple locations, offering the performance, reliability, and availability that businesses need to communicate.

Intelligent Network Integration

The Cisco ASA 5500 Series takes advantage of more than 20 years of Cisco networking leadership and innovation, and delivers a wide range of intelligent networking services for seamless integration into today's diverse network environments. Key network integration services include:

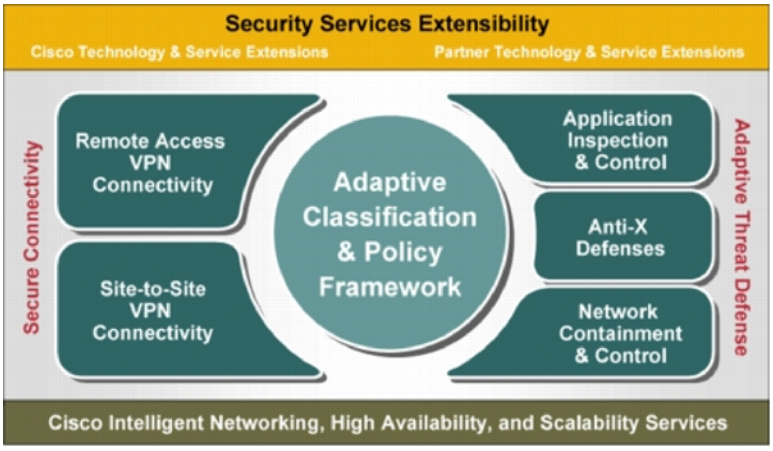
- **Layer 2 transparent firewall**—Provides the ability to rapidly deploy Cisco ASA 5500 Series appliances into existing networks without requiring any addressing changes, and delivers high-performance stealth Layers 2–7 security services and provides protection against network layer attacks with integration in complex routing, high-availability, and multicast environments.
- **Services virtualization**—Enables the logical partitioning of a single Cisco ASA 5500 Series appliance into multiple virtual firewalls, each with its own unique policies and administration; this capability is ideal for enterprises consolidating multiple firewalls into a single Cisco ASA 5500 Series appliance, or for service providers that offer managed firewall or hosting services.
- **Standard 802.1q-based VLAN support**—Provides easy integration into switched network environments.
- **Open Shortest Path First (OSPF) dynamic routing services**—Improve networking resiliency by detecting network outages within seconds, and routing around them.
- **Protocol Independent Multicast (PIM) Sparse Mode v2 and bidirectional PIM routing support**—Provide secure delivery of mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services.
- **IPv6 support**—Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual-stack support of IPv4 and IPv6.
- **Quality of Service (QoS)**—Low-Latency Queuing (LLQ) and Traffic Policing features support applications with demanding QoS requirements, such as voice or video, helping ensure an end-to-end network QoS policy; latency-sensitive traffic can be prioritized ahead of file transfer and other more delay-tolerant traffic.
- **IP phone "zero-touch provisioning" services**—Simplifies IP phone deployments by helping the phones register with the correct Cisco CallManager systems and download any additional configuration information and software images.
- **Resilient architecture**—Provides businesses with both stateful Active/Active and Active/Standby high-availability services, as well as VPN device clustering, to help maximize throughput and network uptime; the Cisco ASA 5500 Series also supports "zero-downtime software upgrades," which allow businesses to install software maintenance releases on failover pairs without affecting connections or network uptime; additionally, integrated dynamic load-balancing capabilities provide high session scalability and resiliency for remote-access VPN deployments.

UNIQUE ADAPTIVE IDENTIFICATION AND MITIGATION SERVICES ARCHITECTURE

Through its unique Adaptive Identification and Mitigation services architecture, the Cisco ASA 5500 Series brings a new level of security and policy control to networks (Figure 1). The AIM architecture allows businesses to adapt and extend the security services profile of the Cisco ASA 5500 Series through highly customizable flow-specific security policies that tailor security needs to application requirements while providing performance and security service extensibility through user-installable SSMs. This adaptable architecture enables businesses deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and anti-x services such as those delivered by the Adaptive Inspection and Prevention (AIP) SSM. Furthermore, the AIM architecture enables the integration of future threat identification and mitigation services, further extending the outstanding investment protection provided by the Cisco ASA 5500 Series, and allowing businesses to adapt their network defenses to new threats as they arise.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Figure 1. Cisco Adaptive Identification and Mitigation Architecture


Security Services Extensibility
Cisco Technology & Service Extensions
Partner Technology & Service Extensions
Secure Connectivity
Remote Access VPN Connectivity
Site-to-Site VPN Connectivity
Adaptive Classification & Policy Framework
Application Inspection & Control
Anti-X Defenses
Network Containment & Control
Adaptive Threat Defense
Cisco Intelligent Networking, High Availability, and Scalability Services

Using the powerful policy framework offered by the Cisco ASA 5500 Series, administrators can orchestrate detailed policies that define what specific services are applied to individual traffic flows. Services include more than 30 different application- and protocol-specific inspection engines, QoS policies, anti-x services, and other inspection and network services. Policies can be based on numerous criteria, including network addresses, traffic types, VPN tunnel, and application or destination target. By enabling the selection of specific security or network services on a per-flow basis, this architecture allows security services to be implemented in a highly granular fashion in support of specific security policies.

REDUCED DEPLOYMENT AND OPERATIONS COSTS

While increasing network security, the Cisco ASA 5500 Series also decreases deployment and operational costs. Its broad VPN and security services profile makes it a single device for many uses, providing platform and management standardization. It can be deployed as a converged threat prevention device by using its access control, application inspection, and worm, virus, and other malware mitigation technologies. It can be used as a dedicated VPN termination device by using its highly scalable site-to-site IPSec and SSL remote-access VPN capabilities. Alternatively, it serves equally well in the network interior for interdepartmental access control and to guard against worms, viruses, and other malicious code that internal users may unwittingly bring into a network. In small business and branch office environments, the Cisco ASA 5500 Series serves as an “all-in-one” solution, offering comprehensive threat prevention and VPN services better suiting the budgets and operational models of such deployments. This adaptive “single platform, many uses” approach reduces the number of platforms that must be deployed and managed. This common operating environment also simplifies configuration, monitoring, troubleshooting, and security staff training. To further minimize operations costs, the Cisco ASA 5500 Series is highly network-aware—it can be inserted gracefully into the network without disrupting legitimate traffic and applications.

Flexible Management Solutions Lower Operations Costs

Cisco ASA 5500 Series adaptive security appliances deliver a wealth of configuration, monitoring, and troubleshooting methods, giving businesses flexibility to use the methods that best meet their needs. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. These appliances additionally provide up to 16 levels of customizable administrative roles, so that businesses can grant administrators and operations personnel the appropriate level of access to each appliance; for example, monitoring only access, read-only access to the configuration, network configuration only, firewall configuration only, and so on.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Next-Generation Centralized Management Solutions

Cisco ASA 5500 Series appliances running Cisco ASA Software Version 7.0 can be centrally managed using the upcoming follow-on software release to CiscoWorks VPN/Security Management Solution (VMS) 2.3. This highly scalable, next-generation, three-tier management solution will include the following features:

- Comprehensive configuration and software image management
- Device hierarchy with “Smart Rules”-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- Intelligent discovery and optimization of security policies and object groups
- “Touchless” software image management for remote Cisco ASA 5500 Series appliances
- Support for dynamically addressed appliances

Attack Mitigation and Event Monitoring Solutions

Network-based attacks can be easily and accurately identified, managed, and eliminated within commercial or enterprise environments using the Cisco Security Monitoring, Analysis, and Response System. Cisco Security Monitoring, Analysis, and Response System appliances analyze and correlate security events, syslog, and NetFlow data from a wide variety of desktop, server, and network security solutions to determine the actual attack path and provide mitigation options, thus simplifying security incident management for environments where dedicated security analysts may not be available.

Additionally, Cisco offers the CiscoWorks Security Information Management Solution (CiscoWorks SIMS), which is well-suited for large enterprises and managed security services providers with dedicated security analysts who require in-depth data collection, forensic analysis, audit and compliance, and reporting for complex, multi-vendor networks.

World-Class Device Management Solutions

The integrated Cisco Adaptive Security Device Manager (ASDM) provides a world-class Web-based management interface that greatly simplifies the deployment, ongoing configuration, and monitoring of a single Cisco ASA 5500 Series appliance—without requiring any software (other than a standard Web browser and Java Plug-In) to be installed on an administrator’s computer. Intelligent setup and VPN wizards provide easy integration into any network environment, and informative monitoring features, including a dashboard and real-time syslog viewer, provide vital device and network health status and event monitoring at a glance.

Alternatively, administrators can remotely configure, monitor, and troubleshoot their Cisco ASA 5500 Series appliances using a command-line interface (CLI). Secure CLI access is available using several methods, including Secure Shell (SSHv2) Protocol, Telnet over IPSec, and out-of-band access through a console port.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

FEATURES AND BENEFITS OF CISCO ASA SOFTWARE VERSION 7.0

Cisco ASA Software Version 7.0 for Cisco ASA 5500 Series adaptive security appliances provides a wealth of features, including those detailed in Table 1. A complete list of features is available in the release notes.

Table 1. Features and Benefits of Cisco ASA Software Version 7.0

Feature	Benefit
Application Security Services	
Advanced Application Inspection and Control Services	• Integrates 30 specialized inspection engines that provide rich application control and security services for protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Extended Simple Mail Transfer Protocol (ESMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), Internet Control Message Protocol (ICMP), SQL*Net, Network File System (NFS), H.323 Versions 1–4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Media Gateway Control Protocol (MGCP), Real-Time Streaming Protocol (RTSP), Telephony Application Programming Interface (TAPI) and Java Telephony Application Programming Interface (JTAPI) over Computer Telephony Interface Quick Buffer Encoding (CTIQBE) protocol, GPRS Tunneling Protocol (GTP), Lightweight Directory Access Protocol (LDAP), Internet Locator Service (ILS), Sun Remote Procedure Call (RPC), and many more
Advanced Web Security Services	• Enables deep inspection services for Web traffic, which provide granular control over HTTP sessions for improved protection from a wide range of Web-based attacks • Gives businesses precise control over what HTTP commands or methods can be used on a per-flow basis (different policy for traffic coming from Internet vs. traffic coming from a staging Web server to production Web server, for example), thus protecting businesses from a variety of Web-based attacks, including unauthorized deletion or modification of Web content • Delivers a wide range of additional powerful HTTP security services, including RFC compliance enforcement, protocol anomaly detection, protocol state tracking, response validation, Multipurpose Internet Mail Extensions (MIME) type validation and content control, Uniform Resource Identifier (URI) length enforcement, and more
Tunneling Application Control	• Provides advanced inspection services to detect and optionally block instant messaging, peer-to-peer file sharing, and other applications tunneling through Web application ports • Blocks popular instant messaging applications such as AOL Instant Messenger, Microsoft Messenger, and Yahoo Messenger • Stops peer-to-peer file sharing applications such as KaZaA and Gnutella • Thwarts tunneling applications such as GoToMyPC
FTP Security Services	• Delivers advanced FTP inspection services, including protocol anomaly detection, protocol state tracking, Network Address Translation (NAT) and Port Address Translation (PAT) support, and dynamic port opening and closing • Gives administrators greater control over the use of numerous FTP commands, allowing them to have the security appliance enforce what operations users and groups can perform within FTP sessions (such as FTP gets and puts) • Provides server obfuscation techniques and additional attack signatures to further protect FTP servers from attack
ESMTP E-Mail Security Services	• Supports ESMTP security inspection services including protocol anomaly detection, protocol state tracking, and support for the following new commands introduced in ESTMP protocol: AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY • Protects businesses from malicious SMTP and ESTMP commands with automatic command filtering
SNMP Security Services	• Delivers SNMP filtering services allowing administrators to maintain a consistent version of the SNMP protocol flowing through their networks • Provides version filtering for all SNMP traffic attempting to flow through a Cisco ASA 5500 Series appliance, supporting filtering of SNMP versions 1, 2, 2c, and 3
ICMP Security Services	• Enables secure usage of ICMP for troubleshooting and improved network performance by providing state tracking services for ICMP connections, as well as providing additional controls for ICMP error messages
Sun RPC and Network Information Service Plus	• Includes support for port-hopping UNIX applications through stateful inspection and NAT services for Sun RPC and NIS+ sessions transactions that use Portmapper v2 or RPCBind v3 or v4

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
(NIS+) Security Services	
3G Mobile Wireless Security Services	• Delivers rich security services for 3G Mobile Wireless environments that provide packet switched data services using the General Packet Radio Service (GPRS) Tunneling Protocol standard (GTP) • Provides advanced GTP inspection services that enable Mobile Wireless providers to have secure interactions with roaming partners through robust filtering capabilities based on GTP specific parameters, such as International Mobile Subscriber Identity (IMSI) prefixes and access point name (APN) values, and more **Note:** This feature is licensed separately.
H.323 Security Services	• Enables advanced H.323 inspection services that support versions 1–4 of the protocol along with Direct Call Signaling (DCS) and Gatekeeper Router Control Signaling (GKRCS) to provide flexible security integration in a variety of H.323-driven voice-over-IP (VoIP) environments • Includes NAT and PAT support for H.323 services, including advanced features such as fax over IP (FoIP) using the T.38 protocol, an ITU standard that defines how to transmit FoIP in real time
SIP Security Services	• Delivers a fortified SIP inspection engine that secures both, UDP and TCP based SIP environments • Enables NAT- and PAT-based address translation support for SIP-based IP phones and applications such as Microsoft Windows Messenger, while delivering advanced services such as call forwarding, call transfers, and more
SCCP Security Services	• Provides secure integration of Cisco SCCP-based IP telephony services with Cisco CallManager Version 4.1 while successfully connecting calls over multiprotocol VoIP environments across NAT and PAT boundaries
MGCP Security Services	• Enables rich MGCP security services and NAT- and PAT-based address translation services for MGCP-based connections between media gateways and call agents or media gateway controllers
RTSP Security Services	• Delivers NAT-based address translation services for RTSP media streams for improved support in real-time networking environments
TAPI/JTAPI over CTIQBE Security Services	• Supports inspection of various Cisco TAPI- and JTAPI-based applications that use CTIQBE, including Cisco IP SoftPhone and the Cisco Customer Response solution
Fragmented and Segmented Multimedia Stream Inspection	• Enables inspection of H.323, SIP, and SCCP-based voice and multimedia streams that have been fragmented or segmented
Advanced TCP Security Engine	• Supports several foundational capabilities to assist in detecting protocol and application layer attacks • Provides TCP stream reassembly and analysis services to help detect attacks that are spread across a series of packets • Offers TCP traffic normalization services for additional techniques to detect attacks, including advanced flag and option checking, TCP packet checksum verification, detection of data tampering in retransmitted packets, and more
Anti-X Security Services	
Advanced Intrusion Prevention and Anti-X Services	• Delivers advanced protection from known and unknown network and application layer attacks, DoS attacks, and malware, including worms, network viruses, Trojan horses, spyware, and adware • Analyzes network traffic accurately for these threats using a wide range of techniques, including stateful pattern recognition, protocol analysis, traffic anomaly detection, protocol anomaly detection, and Layer 2 analysis to detect man-in-the-middle attacks • Provides specialized safeguards to “scrub” network traffic to prevent “detection evasion” attempts, including IP fragmentation reassembly and normalization, TCP stream reassembly and normalization, TCP evasion control, as well as IP antispoofing and deobfuscation services • Helps ensure malicious attacks are stopped without impacting legitimate traffic by using innovative Cisco Risk Rating technology—incorporating four elements (event severity, signature fidelity, asset value, and attack relevancy) to accurately determine the risk of an event, and then confidently performing administrator-specified mitigation action(s) • Provides on-device event correlation capabilities through Cisco Meta Event Generator to quickly identify and stop new threats and optionally reduce the number of events sent to centralized monitoring systems for analysis • Supports both "in-line" prevention of attacks, as well as detection only, of attacks in both routed or Layer 2

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
	transparent bridging modes • Gives administrators granular control over protocols, and provides custom regular expression matching tools for businesses to craft environment-specific signatures • Uses auto-update capability to download the latest threat information from Cisco.com (refer to Cisco Services for IPS for more information) **Note:** These features are available only when an AIP SSM is installed in a Cisco ASA 5500 Series appliance.
Multi-Vector Threat Protection	• Incorporates a variety of technologies to defend businesses from many popular forms of attacks, including DoS attacks, fragmented attacks, replay attacks, and malformed packet attacks • Provides advanced attack protection features such as DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify, and TCP intercept to identify and stop a wide range of attacks • Delivers advanced TCP stream reassembly and traffic normalization services to assist in detecting hidden application and protocol layer attacks
URL Filtering	• Enables robust employee Web usage management and control through integration with Websense- and Secure Computing/N2H2- based URL filtering solutions • Supports HTTPS and FTP Web request filtering through enhanced Websense integration
ActiveX and Java Filtering	• Provides optional filtering of ActiveX and Java applets to prevent downloads of malware and the resulting damage malware can create
Network Containment and Control Services	
Stateful Inspection Firewall Services	• Provides wide range of perimeter network security services to prevent unauthorized network access • Delivers robust stateful inspection firewall services that track the state of all network communications • Provides flexible access-control capabilities for more than 100 predefined applications, services, and protocols, with the ability to define custom applications and services • Supports inbound and outbound access control lists (ACLs) for interfaces, time-based ACLs, and per-user or -group policies for improved control over network and application usage • Simplifies management of security policies by giving administrators the ability to create reusable network and service object groups that can be referenced by multiple security policies, simplifying initial policy definition and ongoing policy maintenance
Access Control Services	• Delivers a flexible solution for defining access control policies by including support for outbound ACLs (in addition to inbound ACLs), allowing access controls to be enforced as network traffic enters or exits an interface • Gives administrators greater control over resource usage by defining time-based ACLs, when certain ACL entries are active, with custom time ranges applied to selected ACLs • Offers a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs without the need to remove and replace ACL entries • Enables the creation of security policies based on interface name instead of IP address, a feature that is especially useful in broadband environments where the external interface is typically assigned a dynamic IP address • Provides powerful reporting and troubleshooting capabilities that help enable collection of detailed statistics on which ACL entries are triggered by network traffic attempting to traverse a security appliance • Gives precise control over which ACL entry-related syslog events are generated • Supports dynamic downloading and enforcement of ACLs on a per-user basis, upon user authentication with the firewall
Object Grouping	• Enables administrators to group network objects (such as devices, networks, and services) into logical groups to greatly simplify access control rule definition and maintenance
NAT and PAT Services	• Provides rich dynamic, static, and policy-based NAT and PAT services • Simplifies deployment of Cisco ASA 5500 Series appliances by eliminating the requirement for address translation policies to be in place before allowing network traffic to flow—now, only hosts and networks that require address translation will need to have address translation policies configured

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
Secure Connectivity Services	
Cisco Easy VPN Server and IPSec Remote-Access Concentrator Services	• Provides market-leading IPSec remote-access VPN concentrator services for up to 5000 simultaneous remote software- or hardware-based VPN clients (on Cisco ASA 5540 appliances with VPN Premium license) • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions (such as the Cisco VPN Client) upon connection, eliminating the need to manage each client separately and therefore helping ensure enforcement of the latest corporate VPN security policies • Performs VPN client security posture checks when a VPN connection attempt is received, including enforcing usage of authorized host-based security products (such as the Cisco Security Agent) • Provides administrators precise control over the types of VPN clients (software client, router, Cisco VPN 3002, and Cisco PIX® Security Appliance) that are allowed to connect based on type of client and version of VPN client software • Supports automatic software updates of Cisco VPN clients and Cisco VPN 3002 hardware clients, with the ability to trigger updates when VPN connections are established, or on demand for currently connected VPN clients • Extends VPN reach into environments using NAT or PAT, through support for the IETF UDP wrapper mechanism for safe traversal through NAT and PAT boundaries as well as Cisco TCP and UDP NAT traversal methods • Allows administrators to require that all traffic from a remote VPN client be sent up to the Cisco ASA 5500 Series appliance, allowing Internet-destined traffic from remote-access user VPN tunnels to leave through the same interface it arrived at (after firewall rules, URL filtering policies, and other security checks have been optionally applied) • Supports Lempel-Ziv Standard (LZS) compression for optimizing performance over low-bandwidth connections
Cisco VPN Client	• Includes a free unlimited license for the highly acclaimed, industry-leading Cisco VPN Client • Available on wide range of platforms, including Microsoft Windows 98, ME, NT, 2000, and XP; Sun Solaris; Intel-based Linux distributions; and Apple Macintosh OS X • Provides many innovative features, including dynamic security policy downloading from Cisco Easy VPN Server-enabled products, automatic failover to back up Easy VPN Servers, administrator customizable distributions, and more • Integrates with the award-winning Cisco Security Agent for comprehensive endpoint security
WebVPN (SSL VPN) Remote-Access Concentrator Services	• Provides SSL VPN-based remote-access connectivity from almost any Internet-enabled location, using only a Web browser and its native SSL encryption • Gives remote users access to network resources from non-corporate-managed machines such as home PCs, Internet kiosks, or wireless hotspots, without relying on preinstalled VPN client software • Supports up to 2500 simultaneous SSL VPN connections (on Cisco ASA 5540 appliances with VPN Premium license) • Allows administrators to customize Web interface for remote-access users • Provides CIFS (Microsoft Windows) file share access through an easy-to-use Web interface • Enforces granular, group-based access control, limiting users to specific network resources • Provides access to TCP-based applications, such as Telnet and Windows Terminal Services, with the SSL-VPN Port Forwarding Java applet (on systems running Sun Java Runtime Environment [JRE] 1.4 or later) **Note:** The WebVPN features in this software release are currently provided as a free trial, and future major software releases will require the purchase and installation of a WebVPN feature license to use these and future WebVPN features.
Remote-Access VPN Clustering and Load Balancing	• Supports improved IPSec and Cisco WebVPN remote-access scalability and reliability through integrated VPN clustering and load-balancing services, with support to join Cisco VPN 3000 Series Concentrator clusters, or create clusters based on the Cisco ASA 5500 Series
Native Integration with Popular User Authentication Services	• Provides convenient method for authenticating VPN users through native integration with popular authentication services, including Microsoft Active Directory, Microsoft Windows Domains, Kerberos, LDAP, and RSA SecurID (without requiring a separate RADIUS or TACACS+ server to act as an intermediary)

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
Site-to-Site VPN Services	• Extends networks securely over the Internet by helping ensure data privacy, data integrity, and strong authentication to remote networks, with support for up to 5000 simultaneous remotely connected sites (on Cisco ASA 5540 appliances that have a VPN Premium license) • Supports Internet Key Exchange (IKE) and IPSec VPN standards with hub-and-spoke or meshed VPN configurations • Improves network reliability and performance through support of OSPF dynamic routing and reverse-route injection over site-to-site VPN tunnels
X.509 Certificate and Certificate Revocation List (CRL) Support	• Supports Simple Certificate Enrollment Protocol (SCEP)-based enrollment and manual enrollment with leading X.509 solutions from Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign • Interoperates with large-scale PKI deployments through n-tiered certificate hierarchy support • Delivers the ability to manually enroll into X.509 certificate authorities through support for Public Key Cryptography Standard (PKCS) #10 formatted certificate requests • Enables the manual importing of certificates using PKCS #7, and importing certificates with private keys using PKCS #12 • Supports a variety of RSA (Rivest, Shamir, Adelmen) key sizes ranging up to 4096 bits • Includes support for DSA (Digital Signature Algorithm)-based X.509 certificates with key sizes ranging up to 1024 bits
High-Availability Services	
Active/Standby Stateful Failover	• Leverages the award-winning stateful failover capabilities of the Cisco PIX Security Appliances to ensure resilient network protection for enterprise network environments • Cisco ASA 5500 Series appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. In the event of a system or network failure, network sessions are automatically transitioned between firewalls, with complete transparency to users
Active/Active Stateful Failover	• Provides a complementary solution to Active/Standby failover, where both systems in an Active/Active failover pair actively pass network traffic simultaneously—effectively doubling the throughput of the failover pair for bursty network traffic conditions • Supports bidirectional state sharing between Active/Active failover pair members for support of advanced network environments with asymmetric routing topologies, allowing flows to enter through one Cisco ASA 5500 Series appliance and exit through the other, if required
VPN Stateful Failover	• Maximizes VPN connection uptime with new Active/Standby stateful failover for VPN connections • Synchronizes all security association state information and session key material between failover pair members, providing a highly resilient VPN solution
LAN-Based Failover	• Enables geographic separation of Cisco ASA 5500 Series appliances in a failover pair by allowing failover information to be shared over a dedicated LAN connection between failover pair members
Zero-Downtime Software Upgrades	• Enables businesses to perform software maintenance release upgrades on Cisco ASA 5500 Series appliance failover pairs without affecting network uptime or connections
Intelligent Networking Services	
Security Contexts	• Enables creation of multiple security contexts (virtual firewalls) within a single Cisco ASA 5500 Series appliance, with each context having its own set of security policies, logical interfaces, and administrative domains • Supports four licensed levels of security contexts: 5, 10, 20, and 50 (the maximum number of contexts supported is based on the Cisco ASA 5500 Series model) • Provides businesses a convenient way of consolidating multiple firewalls into a single physical appliance or failover pair, while retaining the ability to separately manage each of these virtual instances • Enables service providers to deliver resilient multi-tenant firewall services with a pair of redundant appliances **Note:** This feature is licensed separately.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
Layer 2 Transparent Firewall	• Supports deployment of a Cisco ASA 5500 Series appliance in a secure Layer 2 bridging mode, providing rich Layer 2–7 firewall security services for the protected network while remaining "invisible" to devices on each side of it • Simplifies Cisco ASA 5500 Series appliance deployments in existing network environments by not requiring businesses to readdress the protected networks • Supports creation of Layer 2 security perimeters by enforcing administrator-defined Ethertype-based access control policies for Layer 2 network traffic
VLAN-Based Virtual Interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking and multiple VLAN trunks per Cisco ASA 5500 Series appliance • Supports up to 10 VLANs on Cisco ASA 5510 appliances (with the Security Plus license), 25 VLANs on Cisco ASA 5520 appliances, and 100 VLANs on Cisco ASA 5540 appliances
OSPF Dynamic Routing	• Provides comprehensive OSPF dynamic routing services on Cisco ASA 5500 Series appliances using technology based on world-renowned Cisco IOS® Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco ASA 5500 Series NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
Routing Information Protocol (RIP) Dynamic Routing	• Enables secure integration in RIP based enterprise networks by learning routing updates for both versions 1 and 2 of the protocol • Protects against RIP-based reconnaissance activities and DoS attacks by supporting plaintext and keyed-MD5 authentication methods for RIPv2
Multicast Routing	• Streamlines the delivery of multimedia traffic in videoconferencing, collaborative computing, and mission-critical real-time enterprise applications through full PIM Sparse Mode v2 and bidirectional PIM routing support (based on Cisco IOS Software Multicast technology) • Facilitates a wide range of multicast applications by including support for Internet Group Management Protocol (IGMPv2) and stub multicast routing, including NAT and PAT and the ability to build ACLs for multicast traffic
QoS Services	• Delivers per-flow, policy-based QoS services, with support for LLQ and Traffic Policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications • Enables businesses to have end-to-end QoS policies for their extended networks
IPv6 Networking	• Provides access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4 and IPv6 network environments through dual-stack support • Delivers IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP • Supports SSHv2, Telnet, HTTP and HTTPS, and ICMP-based management over IPv6
Security Level per Network Interface	• Leverages the Cisco PIX Security Appliance interface security-level concept to simplify deployment in DMZ environments • Simplifies deployment of Cisco ASA 5500 Series appliances in intranet environments by allowing multiple interfaces to share a common security level, and enabling administrators to define custom security policies for traffic flowing between interfaces at the same security level, without intrinsically permitting any type of automatic traffic flow
Dynamic Host Configuration Protocol (DHCP) Server	• Provides DHCP server services on one or more interfaces, allowing devices to obtain IP addresses dynamically • Includes extensions for automated provisioning of Cisco IP phones and Cisco SoftPhone IP telephony solutions

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
DHCP Relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, helping enable centralized distribution, tracking, and maintenance of IP addresses
Network Time Protocol (NTPv3) Client	• Provides convenient method for synchronizing the clock on Cisco ASA 5500 Series appliances with other devices on a network
Flexible Management Solutions	
Cisco ASDM	• Offers simple, secure remote management of Cisco ASA 5500 Series appliances through world-class, integrated, Web-based GUI • Provides a wide range of informative, real-time, and historical reports that give critical insight into usage trends, performance baselines, and security events
Command Line Interface (CLI)	• Allows customers to use existing Cisco PIX Security Appliance and Cisco IOS Software CLI knowledge for easy installation and management without additional training • Supports improved ease of use with services such as command completion, context-sensitive help, and command aliasing • Accessible through variety of methods, including console port, Telnet, and SSHv2
Cisco Modular Policy Framework	• Provides a powerful, highly flexible framework for defining flow- or class-based policies, enabling administrators to identify a network flow or class based on different conditions, and then apply a set of customizable services to each flow or class • Improves control over applications by introducing the ability to have flow- or class-specific firewall and inspection policies, QoS policies, connection limits and timers, and more
Authentication, Authorization, and Accounting (AAA) Services	• Enables the strong authentication of users through the Cisco ASA 5500 Series appliances through a local user database or through integration with enterprise databases, either directly using TACACS+ and RADIUS or indirectly with Cisco Secure Access Control Server (ACS) • Supports up to 16 levels of customizable administrative roles, so that businesses can grant administrators and operations personnel the appropriate level of access to each appliance; for example, monitoring-only access, read-only access to the configuration, network configuration only, firewall configuration only, and so on • Provides the ability to generate TACACS+ AAA records for tracking administrative access to Cisco ASA 5500 Series appliances, as well as tracking all configuration changes made during an administrative session • Supports sending accounting information to multiple RADIUS servers simultaneously • Enhances network resiliency by giving administrative the ability to dynamically fall back to the local user database in case of external TACACS+ or RADIUS server outages
Cut-Through Proxy Services	• Provides three different methods to optionally authenticate users (over HTTP, HTTPS, or Telnet), which can be required before any network traffic from that user can traverse the Cisco ASA 5500 Series appliance • Uses AAA framework for source of user authentication—authenticating through either the local user database on the appliance or a wide variety of popular third-party authentication services (through TACACS+ or RADIUS integration)
SNMP Monitoring	• Includes support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of Cisco ASA 5500 Series appliances • Provides services such as 64-bit counters (for monitoring the Gigabit Ethernet interfaces) and support for bulk MIB data transfers • Support for many SNMP MIBs, including the SNMPv2 MIB (RFC 1907), the Interfaces Group MIB (RFCs 1573 and 2233), the IP MIB (RFC 2011), and the Entity MIB (RFC 2737) • Provides complete visibility into VPN connections with detailed per-tunnel statistics, including tunnel uptime, bytes and packets transferred, and more, through support for the Cisco IPSec Flow Monitoring MIB

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Feature	Benefit
Flexible Syslog and Security Device Event Exchange (SDEE) Monitoring	• Enables the real time monitoring of the Cisco ASA 5500 Series through the management console or through external syslog servers • Delivers accurate time stamping and numbering of syslog messages while supporting multiple syslog servers over either TCP or UDP as the transport protocol • Provides seven levels of syslog filtering to cater to the monitoring needs of businesses of all sizes • Ensures critical messages are not lost under busy network conditions by providing message buffering locally on the appliance • Supports fine-grain control over syslog messages through a variety of methods, including support for changing priority of syslog messages, the ability to disable specific syslog messages, enabling or suppressing logging on a per-ACL entry (ACE) basis, etc.
Software and Configuration File Import and Export	• Provides the ability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS, or Secure Copy Protocol (SCP) • Supports exporting configuration data through TFTP and SCP for off-device configuration storage
SSH and SCP	• Includes support for using both SSHv1 and SSHv2 to remotely manage Cisco ASA 5500 Series appliances, providing improved compatibility with third-party SSH tools • Provides SCP support as another secure method for transferring files, such as configuration and software images, to and from Cisco ASA 5500 Series appliances
Storage of multiple configurations and software images in flash memory	• Enables administrators to perform configuration rollback and offers the ability to store and use multiple configurations and software images in compact flash memory
Secure Asset Recovery	• Prevents unauthorized access to sensitive configuration data, certificates, and key material stored on Cisco ASA 5500 Series appliances by automatically wiping flash memory contents if an asset recovery or password reset procedure occurs (if preconfigured to do so)
Scheduled System Reloads	• Allows administrators to schedule a reload on a Cisco ASA 5500 Series appliance either at a specific time or at an offset from the current time, making it simpler to schedule network downtime and notify remote-access VPN users of an impending reboot
Dedicated Out-of-Band Management Interface	• Enables businesses to implement the best practice of using out-of-band management for their Cisco ASA 5500 Series appliances, as described in the SAFE Blueprint from Cisco, through the ability to designate the onboard Fast Ethernet 10/100 management interface to act only as an out-of-band management interface
Packet Capture	• Gives administrators powerful troubleshooting capabilities by providing robust packet-capturing facilities on each interface of the Cisco ASA 5500 Series appliance • Supports several methods of accessing captured packets, including through the console, secure Web access, or a file exported to a TFTP server
Extended ICMP Ping Services	• Delivers useful troubleshooting methods through support for IPv6 addresses and extended ICMP options, including data pattern, Don't Fragment (DF) bit, repeat count, datagram size, timeout interval, verbose output, and sweep range of sizes
SMTP E-Mail Alerts	• Provides a convenient method for alerting administrators when critical events are encountered, by sending e-mail alert messages to administrator defined e-mail addresses

PRODUCT LICENSING

Cisco ASA 5500 Series appliances provide licensing options to enable features including security contexts, GTP inspection, strong cryptography, as well as increasing VPN peer capacity and platform capabilities.

Feature Licenses

Security Context Licenses

The Cisco ASA 5520 and 5540 can support up to 10 and 50 security contexts, respectively, where each context has its own separate security policies and administrative domain. These appliances include two contexts by default, and those contexts can be used for either Active/Active high

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

availability or virtual firewall services. Several tiers of security context licenses are available, including 5, 10, 20, and 50 security contexts. This license type and related feature set are not supported on the Cisco ASA 5510.

GTP Inspection License

The Cisco ASA 5520 and 5540 can provide advanced security services for GTP 3G Mobile Wireless environments upon purchase and installation of the GTP Inspection license. This license type and related feature set are not supported on the Cisco ASA 5510.

Encryption Licenses

3DES/AES Encryption License

The Cisco ASA 5500 Series supports two different levels of encryption. By default, all Cisco ASA 5500 Series appliances support 56-bit DES, 56-bit RC4, 512-bit RSA, and 512-bit Digital Signature Algorithm (DSA) encryption algorithms. Customers can optionally order a strong encryption license that adds support for 168-bit Triple Data Encryption Standard (3DES), up to 128-bit RC4, up to 4096-bit RSA, and up to 1024-bit DSA encryption algorithms. A strong encryption license can also be obtained subsequently through Cisco.com, if it was not ordered with the appliance originally.

Platform Licenses

Cisco ASA 5510 Adaptive Security Appliance Security Plus License

Businesses can significantly extend the capabilities of the Cisco ASA 5510 by purchasing and installing a Security Plus license. This license increases port density on the platform by enabling the fourth Fast Ethernet port and removing the restriction on the out-of-band management port so that it can be repurposed to a general traffic port, if desired. Integration into switched network environments is simplified with this license, as support for up to 10 VLANs is enabled. Furthermore, this upgrade license maximizes business continuity by enabling Active/Standby high-availability services and triples VPN capacity by supporting up to 150 concurrent VPN connections from mobile users, remote sites, and business partners.

Cisco ASA 5520 Adaptive Security Appliance VPN Plus License

Businesses can extend the IPSec and SSL VPN capacity of their Cisco ASA 5520 with a VPN Plus license, which more than doubles the platform VPN capacity to support up to 750 concurrent VPN connections from mobile users, remote sites, and business partners.

Cisco ASA 5540 Adaptive Security Appliance VPN Plus and VPN Premium Licenses

Businesses have multiple options for extending the IPSec and SSL VPN capacity of their Cisco ASA 5540. With a VPN Plus license, businesses quadruple the platform base VPN capacity to support up to 2000 concurrent IPSec VPN and 1250 WebVPN connections from mobile users, remote sites, and business partners. This license maximizes the platform VPN capacity, and offers 10 times the capacity of the base platform, supporting up to 5000 concurrent IPSec VPN and 2500 WebVPN connections.

PRODUCT SPECIFICATIONS

Tables 2–4 provide information on compatibility between Cisco ASA 5500 Series appliances and VPN clients, VPN products, and certain cryptographic standards.

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Cisco VPN Client Compatibility

Cisco ASA 5500 Series appliances support numerous software- and hardware-based Cisco VPN clients, including those listed in Table 2.

Table 2. Compatibility Between Cisco ASA 5500 Series Appliances and VPN Clients

VPN Client	Versions Supported
Software IPSec VPN Clients	• Cisco VPN Client for Windows, Version 3.6 and later • Cisco VPN Client for Linux, Version 3.6 and later • Cisco VPN Client for Solaris, Version 3.6 and later • Cisco VPN Client for Mac OS X, Version 3.6 and later
Hardware IPSec VPN Clients (Cisco Easy VPN Remote)	• Cisco VPN 3002 Hardware Client, Version 3.0 and higher • Cisco IOS Software Easy VPN Remote, Release 12.2(8)YJ • Cisco PIX Security Appliance Software versions 6.2 and 6.3

Cisco Site-to-Site VPN Compatibility

In addition to providing interoperability for many third-party VPN products, Cisco ASA 5500 Series appliances interoperate with the Cisco VPN products listed in Table 3 for site-to-site VPN connectivity:

Table 3. Site-to-Site VPN Compatibility Between Cisco ASA 5500 Series and VPN Products

VPN Gateway	Versions Supported
Cisco ASA 5500 Series Appliances	Cisco ASA Software Version 7.0(1) and later
Cisco IOS Software Routers	Cisco IOS Software Release 12.1(6)T and later
Cisco PIX Security Appliances	Cisco PIX Security Appliance Software Version 6.0(1) and later
Cisco VPN 3000 Series Concentrators	Cisco VPN 3000 Series Concentrator Software Version 3.0 and later

Cryptographic Standards Supported

Cisco ASA 5500 Series appliances support numerous cryptographic standards and related third-party products and services (Table 4).

Table 4. Cryptographic Standards and Products Supported by Cisco ASA 5500 Series

Cryptographic Standard	Key Lengths and Hash Sizes Supported
Asymmetric (public key) Encryption Algorithms	• RSA public/private key pairs, 512 to 4096 bits • DSA public/private key pairs, 512 to 1024 bits
Symmetric Encryption Algorithms	• Advanced Encryption Standard (AES): 128, 192, and 256 bits • DES: 56 bits • 3DES: 168 bits • RC4: 40, 56, 64, and 128 bits
Perfect Forward Secrecy (Diffie-Hellman key negotiation)	• Group 1: 768 bits • Group 2: 1024 bits • Group 5: 1536 bits • Group 7: 163 bits (Elliptic Curve Diffie-Hellman)

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Cryptographic Standard	Key Lengths and Hash Sizes Supported
Hash Algorithms	• Message Digest Algorithm (MD5): 128 bits • Secure Hash Algorithm 1 (SHA-1): 160 bits
X.509 Certificate Authorities	• Baltimore UniCERT • Cisco IOS Software • Entrust Authority • iPlanet/Netscape CMS • Microsoft Certificate Services • RSA KEON • VeriSign OnSite
X.509 Certificate Enrollment Methods	• Simple Certificate Enrollment Protocol (SCEP) • Manual (PKCS #7 and #10)

SYSTEM REQUIREMENTS

Table 5 lists system requirements for Cisco ASA 5500 Series appliances running Cisco ASA Software Version 7.0.

Table 5. System Requirements

System Requirement	Description
Platforms Supported	• Cisco ASA 5510 Adaptive Security Appliance • Cisco ASA 5520 Adaptive Security Appliance • Cisco ASA 5540 Adaptive Security Appliance
Minimum RAM	• Cisco ASA 5510: 256 MB • Cisco ASA 5520: 512 MB • Cisco ASA 5540: 1024 MB
Minimum System Flash Memory	• 64 MB
Expansion Cards Supported	• Cisco AIP SSM • AIP SSM 10 • AIP SSM 20

ORDERING INFORMATION

To place an order, visit the Cisco Ordering Home Page or refer to Table 6.

Table 6. Ordering Information

Product Name	Part Number
Cisco ASA 5500 Series 5 Security Contexts license	ASA5500-SC-5=
Cisco ASA 5500 Series 10 Security Contexts license	ASA5500-SC-10=
Cisco ASA 5500 Series 20 Security Contexts license	ASA5500-SC-20=
Cisco ASA 5500 Series 50 Security Contexts license	ASA5500-SC-50=
Cisco ASA 5500 Series 5 to 10 Security Contexts license upgrade	ASA5500-SC-5-10=
Cisco ASA 5500 Series 10 to 20 Security Contexts license upgrade	ASA5500-SC-10-20=
Cisco ASA 5500 Series 20 to 50 Security Contexts license upgrade	ASA5500-SC-20-50=

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Product Name	Part Number
Cisco ASA 5500 Series GTP/GPRS Inspection license	ASA5500-GTP=
Cisco ASA 5510 Adaptive Security Appliance Security Plus license	ASA5510-SEC-PL=
Cisco ASA 5520 Adaptive Security Appliance VPN Plus license	ASA5520-VPN-PL=
Cisco ASA 5540 Adaptive Security Appliance VPN Plus license	ASA5540-VPN-PL=
Cisco ASA 5540 Adaptive Security Appliance VPN Premium license	ASA5540-VPN-PR=
Cisco ASA 5540 Adaptive Security Appliance VPN Plus-to-Premium license upgrade	ASA5540-VPN-PL-PR=

TO DOWNLOAD THE SOFTWARE

Visit the Cisco Software Center to download Cisco ASA Software (Table 7).

Table 7. Software Images for the Cisco ASA 5500 Series

Product Name
Cisco ASA Software Version 7.0
Cisco Adaptive Security Device Manager Version 5.0

SERVICE AND SUPPORT

Cisco offers a wide range of services programs to accelerate customer success. These innovative service programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, refer to Cisco Technical Support Services and Cisco Advanced Services; for services specific to IPS features delivered through the Cisco AIP SSM, refer to Cisco Services for IPS.

FOR MORE INFORMATION

For more information, visit the following links:

- Cisco ASA 5500 Series appliances: http://www.cisco.com/go/asa
- Cisco ASDM: http://www.cisco.com/go/asdm
- CiscoWorks VMS: http://www.cisco.com/go/vms
- Cisco Secure ACS: http://www.cisco.com/go/acs
- SAFE Blueprint from Cisco: http://www.cisco.com/go/safe

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

205226.G_ETMG_KM_6.05

Printed in the USA

© 2005 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.